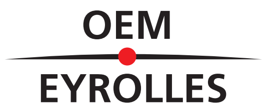
Halte aux hackers

4e édition

Stuart McClure
Joel Scambray
George Kurtz

ISBN : 2-7464-0486-9



Avant-propos

L'ignorance, voilà l'ennemi (bis)

« Contrôlez vos passions, faute de quoi elles se vengeront sur vous. »

Epictète (vers 50-125), philosophe grec stoïcien

« Apprenez-vous vraiment aux gens à pirater un système ? ». Cette question revient constamment, et nous répondons invariablement : « Oui, d'une certaine manière. Nous présentons les techniques et la mentalité des hackers. Nous expliquons ce qu'ils font et comment ils le font. Nous démystifions l'art du piratage pour vous donner les moyens de vous défendre contre ces attaques. Si nous ne faisons pas tomber ces murs, la sécurité des systèmes ne sera jamais qu'illusion. » On nous demande aussi : « Les chances sont-elles du côté des hackers ? ». À cela, nous ne pouvons que répondre par un oui catégorique. Si nous comptabilisons uniquement le temps passé à battre en brèche la sécurité d'un système, le hacker a assurément l'avantage (le nombre de canettes de bière vides en donne un indice fiable). Mais grâce à des livres comme celui-ci et aux informations qu'il apporte, la balance ne penche plus du côté des hackers.

Mais quel est le sens de notre propos ici ? Bien sûr, la sécurité est un sujet difficile et les informations sur les techniques de piratage et les parades appropriées sont encore plus dures à trouver, mais où en sommes-nous aujourd'hui ? Le monde technologique dans lequel nous évoluons manque cruellement d'informations sur les attaques réseau, celles des systèmes d'exploitation, des bases de données et des applications. Rares en fait sont les administrateurs qui comprennent véritablement les enjeux autour de la sécurité et qui savent s'attaquer à ce défi titanesque. Ils doivent combattre des hackers qui connaissent tout des vulnérabilités et des moyens de les exploiter. Qui a l'avantage dans ces conditions ?

Autant se l'avouer : les hackers connaissent toutes ces informations et nous ne leur apprendrons rien de nouveau. Notre objectif est simplement de donner au lecteur un aperçu de leur façon de penser et de travailler. Si vous ne trouvez pas judicieuse la publication des informations présentes dans ce livre, essayez d'imaginer dans quelle situation vous vous trouveriez sans elles : les pirates seraient les seuls à les connaître, alors que vous seriez dans l'ignorance la plus totale. Voulez-vous prendre ce risque ?

Au cas où il vous resterait des doutes quant à l'objectif visé par cet ouvrage, répétons-le encore une fois : n'utilisez ces informations que dans un but louable. Si vous ne suivez pas ce conseil, vous nous trouverez sur votre route et ce ne sera pas une partie de plaisir… pour vous.

Quoi de neuf dans la quatrième édition ?

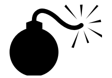
Le monde numérique évolue plus vite que la pensée. Les hackers mettent au point de nouveaux outils, de nouvelles techniques et méthodes à chaque heure du jour et de la nuit. Les recenser, les faire connaître et les expliquer représente un formidable défi. Comme dans les éditions précédentes, nous nous sommes appliqués à vous proposer ce qui se fait de mieux et de plus récent en la matière.

Parmi les nouveautés de cette quatrième édition, on notera plus particulièrement :

1. **Un chapitre entièrement nouveau** traitant des attaques des réseaux sans fil 802.11.
2. **Les dernières méthodes de piratage des réseaux**, notamment l'utilisation de traceroute, dsniff, linsniff, ARP, SNMP, RIP.
3. Des parades mises à jour pour contrer les attaques exploitant les **vulnérabilités des proxy et des pare-feu à filtrage de paquets.**
4. Un **chapitre entièrement refondu consacré au piratage du Web** et mis à jour de façon à traiter des dernières vulnérabilités spécifiques aux différentes plates-formes, d'Apache à IIS, et des techniques les plus courantes, notamment les attaques de cross-site scripting, de fuzzing et les insertions SQL, ainsi que des derniers outils, d'Achilles à Nikto.
5. Une analyse de toutes les ruses et des nouveaux outils de **déni de service distribué (DDoS)**.
6. De nouvelles informations sur les **risques liés aux applications Web**, notamment les problèmes de validation d'entrées et les défauts de conception.
7. **De nouvelles études de cas e**n début de chaque partie, relatant sur une attaque récente.
8. De nouvelles techniques pour **obtenir un accès interdit** à Windows 9*x*/Me/XP et Windows NT/2000/2003 Server, Novell 6, UNIX, Linux et des dizaines d'autres plates-formes.
9. De nouvelles stratégies *préventives* pour vous **défendre contre** les attaques par le réseau commuté de vos PABX, systèmes de messagerie vocale et réseaux privés virtuels.
10. **Le célèbre site Web d'accompagnement (en anglais) sur** http://www.hackingexposed.com avec des liens vers tous les outils et ressources Internet cités dans ce livre.

Conventions utilisées dans cet ouvrage

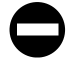
Pour cette quatrième édition, nous avons conservé le format habituel de la série des *Halte aux hackers*. Chaque technique d'attaque est signalée par une icône spécifique placée en marge comme suit :



Cette icône signale une attaque

Vous pouvez ainsi identifier plus aisément les outils et les méthodes spécifiques aux essais d'intrusion.

- Chaque attaque est contrée par des astuces pratiques, adaptées et testées sur le terrain, qui sont également signalées par une icône spécifique.



Cette icône signale une parade

Vous pouvez, si vous le souhaitez, régler immédiatement le problème que nous vous signalons.

- Nous avons également effectué un nettoyage global des exemples de listings de code, des captures d'écran et des diagrammes en veillant, notamment, à rendre plus visibles les entrées des utilisateurs qui apparaissent désormais en gras dans les listings de code.
- Chaque attaque est accompagnée d'un « niveau de risque » qui a été réévalué selon trois facteurs basés sur l'expérience combinée des auteurs :

Popularité	Fréquence d'utilisation globale contre des cibles réelles, où 1 indique une utilisation rare et 10 une utilisation très répandue.
Simplicité	Niveau de compétence nécessaire pour mener à bien l'attaque, où 1 indique une compétence faible, voire aucune compétence, et 10 correspond aux compétences d'un programmeur chevronné.
Impact	Dommages potentiellement provoqués par une exécution réussie de l'attaque, où 1 correspond à la collecte d'informations sans importance sur la cible et 10 correspond à l'accès à un compte de superutilisateur ou à une opération équivalente.
Risque	Moyenne des trois valeurs précédentes calculée afin d'obtenir un niveau de risque global arrondi à l'entier supérieur.

À vous tous

Comme d'habitude, nous nous sommes efforcés de vous fournir des informations à jour, précises et originales sur les techniques et les outils employés par les hackers, ainsi que sur les parades à votre disposition. Nous espérons que vous trouverez dans ce livre des informations de qualité, au-delà des simples trucs et astuces. Notre seul espoir : vous aider à trouver des raisons profondes et fondamentales qui vous inciteront à sécuriser correctement votre réseau contre les Bonnie & Clyde des temps modernes. Bonne lecture à tous !

Mode d'emploi d'un piratage réussi

